ELSEVIER

Theoretical Computer Science 216 (1999) 395–397

Theoretical Computer Science

Note

A shorter proof to uniqueness of solutions of equations[1]

Mingsheng Ying *

Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

Received January 1998; revised June 1998
Communicated by M. Nivat

Abstract

We give a very short proof of uniqueness of solutions of equations regarding observation congruence, the main notion of equality, over Milner's process calculus.

Keywords: Process calculus; Observation congruence; Bisimulation up to bisimilarity; Solutions of equations

Uniqueness of solutions of equations with respect to observation congruence in Milner's process calculus is a very important result and it has many significant applications (for examples, see [1, Chs. 5 and 6]. The purpose of this short note is to give an easier proof of this result.

First, for convenience, we display some definitions and lemmas needed in the sequel.

Definition 1 (cf. Milner [3, p. 3, lines 5–8]). S is a (weak) bisimulation up to $\approx$ if PSQ implies, for all α,

(i) Whenever $P \stackrel{\alpha}{\Rightarrow} P'$ then, for some Q', $Q \stackrel{\widehat{\alpha}}{\Rightarrow} Q'$ and $P' \approx S \approx Q'$.

(ii) Whenever $Q \stackrel{\alpha}{\Rightarrow} Q'$ then, for some P', $P \stackrel{\widehat{\alpha}}{\Rightarrow} P'$ and $P' \approx S \approx Q'$.

The following lemma is necessary in the proof of Proposition 3, but it is also of significance independently.

* E-mail: ying@theory.cs.tsinghua.edu.cn.

[1] This work was supported by National Foundation of Natural Sciences (No: 69725004 and 19671038) and Research and Development Project of Hi-Technology (No: 863-306-05-05-3B) of China and Fok Ying-Tung Education Foundation.

0304-3975/99/$ – see front matter
PII: S0304-3975(98)00187-X

Lemma 1. *Let S be such that PSQ implies, for all α,*

(i) *Whenever $P \xrightarrow{\tau^p} \xrightarrow{\alpha} P'$ $(p \geqslant 0)$ then, for some Q', $Q \stackrel{\widehat{\alpha}}{\Rightarrow} Q'$ and $P' \approx S \approx Q'$,*

(ii) *Whenever $Q \xrightarrow{\tau^p} \xrightarrow{\alpha} Q'$ $(p \geqslant 0)$ then, for some P', $P \stackrel{\widehat{\alpha}}{\Rightarrow} P'$ and $P' \approx S \approx Q'$.*

Then S is a bisimulation up to $\approx$.

Proof. Suppose that $P \xrightarrow{\tau^p} P_1 \xrightarrow{\alpha} P_1' \xrightarrow{\tau^q} P'$ for some $p \geqslant 0$ and $q > 0$. We want to show that for some Q', $Q \stackrel{\widehat{\alpha}}{\Rightarrow} Q'$ and $P' \approx S \approx Q'$. From the condition, we have some Q_1' such that $Q \stackrel{\widehat{\alpha}}{\Rightarrow} Q_1'$ and $P_1' \approx USV \approx Q_1'$ for some U and V. Thus, for some $r \geqslant 0$ and U', it holds that $U \xrightarrow{\tau^r} U'$ and $P' \approx U'$. If $r = 0$, then $P' \approx U' \equiv USV \approx Q_1'$ and it suffices to take $Q' \equiv Q_1'$. If $r > 0$, then $U \xrightarrow{\tau^{r-1}} \xrightarrow{\tau} U'$ and the condition asserts that there must be some V' such that $V \stackrel{\varepsilon}{\Rightarrow} V'$ and $U' \approx S \approx V'$. Again, we can find some Q' with $Q_1' \stackrel{\varepsilon}{\Rightarrow} Q'$ and $V' \approx Q'$. Then $Q \stackrel{\widehat{\alpha}}{\Rightarrow} Q'$ and $P' \approx U' \approx S \approx V' \approx Q'$. □

Definition 2 (cf. Milner [1, Definition 7.4]). X is sequential in E if every subexpression of E which contains X, apart from X itself, is of the form $\alpha.F$ or $\sum \widetilde{F}$.

Definition 3 (cf. Milner [1, Definition 7.5]). X is guarded in E if each occurrence of X is within some subexpression of E of the form $l.F$.

Lemma 2 (cf. Milner [1, Lemma 7.12]). *Let G be guarded and sequential, $vars(G) \subseteq \widetilde{X}$, and let $G\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\alpha} P'$. Then there is an expression H such that $G \xrightarrow{\alpha} H$, $P' \equiv H\{\widetilde{P}/\widetilde{X}\}$ and, for any $\widetilde{Q}$, $G\{\widetilde{Q}/\widetilde{X}\} \xrightarrow{\alpha} H\{\widetilde{Q}/\widetilde{X}\}$. Moreover H is sequential, $vars(H) \subseteq \widetilde{X}$, and if $\alpha = \tau$ then H is also guarded.*

The main result in [1, Section 7.3] is the following

Proposition 3 (cf. Milner [1, Proposition 7.13]). *Let $\widetilde{E}$ be guarded and sequential expressions with free variables $\subseteq \widetilde{X}$, and let $\widetilde{P} = \widetilde{E}\{\widetilde{P}/\widetilde{X}\}$, $\widetilde{Q} = \widetilde{E}\{\widetilde{Q}/\widetilde{X}\}$. Then $\widetilde{P} = \widetilde{Q}$.*

The original proof of the above proposition given in [1], pp. 158–160 is quite tricky and complicated. Here, we present a much shorter and more straightforward proof of this proposition:

Proof. We set

$$S = \{(G\{\widetilde{P}/\widetilde{X}\}, G\{\widetilde{Q}/\widetilde{X}\}) : G \text{ is guarded and sequential, and } vars(G) \subseteq \widetilde{X}\}.$$

(1) By using Lemma 2 repeatedly (especially noting that "if $\alpha = \tau$ then H is also guarded"), we know that for any guarded and sequential G with $vars(G) \subseteq \widetilde{X}$,

(i) if $G\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\tau^p} \xrightarrow{\alpha} P'$, then there exists a sequential H such that $P' \equiv H\{\widetilde{P}/\widetilde{X}\}$ and $G\{\widetilde{Q}/\widetilde{X}\} \xrightarrow{\tau^p} \xrightarrow{\alpha} H\{\widetilde{Q}/\widetilde{X}\}$; and

(ii) if $G\{\widetilde{Q}/\widetilde{X}\} \xrightarrow{\tau^p} \xrightarrow{\alpha} Q'$, then there exists a sequential H such that $Q' \equiv H\{\widetilde{Q}/\widetilde{X}\}$ and $G\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\tau^p} \xrightarrow{\alpha} H\{\widetilde{P}/\widetilde{X}\}$.

Noticing [1, Proposition 7.7] and that H is sequential, $\widetilde{E}$ is guarded and sequential, and $H\{\widetilde{E}/\widetilde{X}\}$ is also guarded and sequential, we obtain $H\{\widetilde{P}/\widetilde{X}\} = H\{\widetilde{E}\{\widetilde{P}/\widetilde{X}\}/\widetilde{X}\} \equiv H\{\widetilde{E}/\widetilde{X}\}\{\widetilde{P}/\widetilde{X}\} S H\{\widetilde{E}/\widetilde{X}\}\{\widetilde{Q}/\widetilde{X}\} \equiv H\{\widetilde{E}\{\widetilde{Q}/\widetilde{X}\}/\widetilde{X}\} = H\{\widetilde{Q}/\widetilde{X}\}$. Thus, with [1, Proposition 7.4] we can assert that

(i)′ if $G\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\tau^p} \xrightarrow{\alpha} P'$, then there exists Q' such that $G\{\widetilde{Q}/\widetilde{X}\} \xrightarrow{\tau^p} \xrightarrow{\alpha} Q'$ and $P' \approx S \approx Q'$; and

(ii)′ if $G\{\widetilde{Q}/\widetilde{X}\} \xrightarrow{\tau^p} \xrightarrow{\alpha} Q'$, then there exists P' such that $G\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\tau^p} \xrightarrow{\alpha} P'$ and $P' \approx S \approx Q'$.

(2) From Lemma 1, [1, Proposition 5.6] and (1) we know that S is a bisimulation up to $\approx$ and for any guarded and sequential G with $vars(G) \subseteq \widetilde{X}$,

(i)″ if $G\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\alpha} P'$, then there exists Q' such that $G\{\widetilde{Q}/\widetilde{X}\} \xrightarrow{\alpha} Q'$ and $P' \approx Q'$; and

(ii)″ if $G\{\widetilde{Q}/\widetilde{X}\} \xrightarrow{\alpha} Q'$, then there exists P' such that $G\{\widetilde{P}/\widetilde{X}\} \xrightarrow{\alpha} P'$ and $P' \approx Q'$.

This means that $G\{\widetilde{P}/\widetilde{X}\} = G\{\widetilde{Q}/\widetilde{X}\}$.

(3) For any $X_i \in \widetilde{X}$, E_i is guarded and sequential. Thus, $P_i = E_i\{\widetilde{P}/\widetilde{X}\} = E_i\{\widetilde{Q}/\widetilde{X}\} = Q_i$ (see [1, Proposition 7.5]), and $\widetilde{P} = \widetilde{Q}$. □

References

[1] R. Milner, Communication and Concurrency, Prentice-Hall, New York, 1989.

[2] R. Milner, Errata in the book Communication and Concurrency, private communication, Edinburg, November, 1990.

[3] R. Milner, A calculus of communicating systems, Lecture Notes in Computer Science, vol. 92, Springer, Berlin, 1980.